Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

ADENDO AO EDITAL DE PREGÃO ELETRÔNICO Nº 022/2022/MTI

EDITAL Nº 022/2022/MTI – PUBLICADO EM 20/10/2022 – PÁG 86 – D.O Nº 28.356

O Diretor Presidente Interino da Empresa Mato-grossense de Tecnologia da Informação - MTI, torna público o ADENDO AO EDITAL DE PREGÃO ELETRÔNICO N. º 022/2022/MTI – Processo MTI-PRO-2022/00404.

OBJETO: Contratação de empresa especializada para fornecimento de licenciamento ou subscrição de SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES PRIVILEGIADAS, incluindo a IMPLANTAÇÃO, ATUALIZAÇÃO E GARANTIA, TREINAMENTO E SERVIÇOS DE MANUTENÇÃO, SUPORTE TÉCNICO E OPERAÇÃO ASSISTIDA pelo prazo mínimo de 36 meses, para atender às demandas da MTI - Empresa Mato-Grossense de Tecnologia da Informação, conforme especificações técnicas e demais condições constantes no Termo de Referência nº 04/2022

EDITAL

1- **Onde se lê:**

13.17. Declarações que devem ser enviadas obrigatoriamente junto com os documentos de habilitação

j) Declaração da MTI no processo quanto ao cumprimento da verificação dos incisos I e II, do art. 38, da Lei 13.303/2016;

2- **Lê se:**

Excluído o item j)

ANEXO I – TERMO DE REFERÊNCIA

3. **Onde se lê:**

ANEXO I – ESPECIFICAÇÃO TÉCNICA SOLUÇÃO

	ANEXO I - ESPECIFICAÇÃO TÉCNICA SOLUÇÃO
SUBITEM	**FUNCIONALIDADE**
Requisitos Funcionais Obrigatórios	

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

1.	**Oferecer acesso segmentado (especificidade usuário + senha)** A solução de cofre de senhas deve permitir a definição detalhada dos privilégios (granularidade) concedidos a um usuário ou grupo específico no ativo ou recurso protegido. Apenas administradores da solução ou usuários por ele delegados poderão efetuar a inclusão, alteração e exclusão destes privilégios.
2.	**Dispor de integração ao Microsoft Active Directory e serviço LDAP** A solução de cofre de senhas deve permitir a autenticação de usuários em domínios Microsoft Active Directory e serviços de diretório no padrão LDAP, de forma integrada e transparente, observando as características de grupamento destes usuários (unidade organizacional/OU). Necessário suportar estes servidores e domínios nas versões especificadas no **quadro 2 (Integração com ativos e produtos utilizados na MTI).**
3.	**Dispor de cofre de senhas inacessível ao usuário final e não-legível para além do domínio da aplicação** A solução de cofre de senhas deve manter o conjunto de senhas (tanto de usuários finais como dos ativos e recursos protegidos) em estado criptografado, inacessível aos usuários finais e aos próprios ativos e recursos protegidos, em uma base que não possa ser utilizada caso copiada para além da própria solução. Todavia, deve dispor de uma forma segura para manter cópias de segurança das contas e configurações da solução.
4.	**Efetuar registro individual do acesso por usuário (ainda que para um único par usuário/senha de um ativo/recurso protegido)** Ainda que o acesso ao ativo/recurso protegido se dê por um único par usuário/senha, a solução deve prover um registro individual por usuário final nela autenticado, a cada sessão. Este registro deverá indicar o período em que o usuário final manteve esta sessão e sua identidade, no mínimo, com fins de manter a rastreabilidade e a pessoalidade das sessões autenticadas.
5.	**Possuir capacidade de fornecer dados de acesso a aplicações e bancos de dados de forma segura.** A solução será capaz de fornecer acesso a aplicações desenvolvidas nas tecnologias e ambientes utilizados na empresa descritos no **quadro 2 (Integração com ativos e produtos utilizados na MTI),** seja entre aplicações ou entre estas e as soluções de bancos de dados listadas no mesmo quadro. Assim, a obtenção dos dados de autenticação entre as aplicações para troca de informações, ou para o acesso ao

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

	banco de dados, será efetuado através da solução de cofre de senhas, não exigindo dos desenvolvedores e mantenedores das aplicações o conhecimento das reais contas e senhas utilizadas nestes ativos/recursos protegidos.
6.	**Deve automatizar o ciclo de vida das contas e senhas geradas para os ativos protegidos, bem como permitir a gestão simplificada do ciclo de vida das contas e senhas dos usuários finais, através de políticas definíveis.** O ciclo de vida das senhas será automatizado (criação, renovação, expiração, rotação) de forma transparente e gerenciável, fazendo uso de senhas geradas randomicamente se assim requisitado, com a complexidade e periodicidade definidas por políticas configuráveis. Igualmente, deve permitir a gestão simplificada do ciclo de vida das contas e senhas dos usuários finais, também sujeitando-as a políticas configuráveis, quanto à sua criação, duração, renovação, expiração e exclusão. A definição destas políticas deve ser restrita aos administradores da solução ou aos usuários por eles delegados a esta função.
7.	**Prover recursos de auditoria e rastreabilidade do uso das credenciais** A solução proverá trilhas de auditoria, visando a rastreabilidade das ações executadas nas sessões por ela autenticadas. Os registros de auditoria e log devem ser invioláveis, sendo possível definir qual sua granularidade de acordo com a sessão e o usuário ou grupo de usuários autenticados, através de políticas configuráveis. Estas trilhas de auditoria devem ser armazenadas em formato criptografado, e deve ser garantida sua inviolabilidade e sua acessibilidade apenas aos administradores da solução ou usuários por eles delegados.
8.	**Possuir aderência da própria ferramenta e auxiliar na obtenção da aderência do conjunto de ativos e recursos protegidos à legislação nacional.** Deve implementar e auxiliar a implementar nas aplicações e ambiente protegidos pela solução à legislação nacional (LGPD, Lei Federal Brasileira nº 13709 de 2018).
9.	**Deve oferecer formas de single-sign-on, login único para mais de um recurso ou ativo protegido** Deve oferecer recursos de single-sign-on, onde uma única autenticação na solução de cofre de senhas permitiria o login seguro, identificado e rastreável, aos ativos protegidos habilitados para determinado usuário final. A partir desta autenticação, as sessões nos ativos e recursos protegidos irão se desenvolver conforme as permissões e políticas configuradas, tanto para o ativo/recurso específico como para o usuário autenticado.

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

10.	**Possuir recursos de análise proativa de ameaças.** A solução deve oferecer relatórios e indicações automatizadas, de forma proativa, de possíveis ameaças e irregularidades no uso das sessões por ela protegidas. Tal funcionalidade deve ser amplamente configurável em seu escopo e granularidade, tanto na aquisição como no tratamento das informações coletadas.
11.	**Deve oferecer appliances hardenizados.** Tanto appliances quanto sistemas operacionais que compõe a solução devem seguir padrões de "hardening" atualizados constantemente pelo fabricante da solução de cofre de senhas e protegidos com firewall interno e detecção de intrusão; Utilizar um banco de dados com as melhores práticas de segurança, deve estar em ambiente "hardenizado", com mecanismo de blindagem e criptografia do sistema operacional e documentação que comprove a contemplação destes requisitos;
12	**Criptografia do banco de dados** Possibilitar a utilização de criptografia do banco de dados utilizado pela solução, para armazenar as senhas das credenciais gerenciadas por ela, devendo ainda ser compatível com pelo menos um dos seguintes métodos e padrões de criptografia: a) AES com chaves de 256 bits; b) FIPS 140-2; c) Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada."
13	**Backup/Restore** O backup/restore de todos os dados e configurações da solução deve estar incluso e deve permitir ao administrador agendar backups para determinada data e hora e exportá-los para um servidor SFTP remoto.
14	**Gerenciamento do ambiente sem agente** Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;
15	**Gerenciamento de certificados digitais** A ferramenta deverá cuidar do ciclo de vida completo de um certificado, possuindo as seguintes funcionalidades: Criação de uma requisição, assinatura, renovação e revogação de certificados
16	**Arquitetura básica** A solução deve ser baseada em appliance físico, atendendo as seguintes especificações: Caso o banco de dados e/ou Sistema Operacional utilizado seja de terceiros (exemplo: ORACLE/SQL ou Windows), a solução deverá ser entregue com licenças de software e garantia que a compatibilize com a solução;

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

	Os usuários geridos pela solução poderão estar conectados simultaneamente; O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é ativo/ativo. A solução deve permitir o gerenciamento e monitoramento de sessões estabelecidas via protocolos: HTTP, HTTPS, SSH e RDP, seja via Proxy ou Jump Server.
17	**Implementar gestão da identidade do usuário final com recursos de autenticação em duas etapas (2FA)** Deve disponibilizar recursos de duplo fator de autenticação para o usuário final, nas formas de mensagem de e-mail, SMS, aplicação para smartphone nos padrões Android e IOS. O código (token) enviado deve possuir tempo de vida pré-determinado, e a exigência de autenticação por duplo fator deve ser configurável na política de autenticação para cada recurso/ativo protegido.
18	**Descoberta de credenciais** Oferecer a funcionalidade de "Discovery" para realizar busca de novas credenciais, certificados além de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos incluindo a possibilidade de descobrir certificados SSL utilizado nos dispositivos gerenciados; A solução deve ser capaz de encontrar dispositivos de rede e credenciais, de no mínimo os seguintes ambientes: a) Servidores Linux/Unix, Windows e VMWare; b) Base de dados Oracle, SQL e MySQL; c) Dispositivos de rede como firewalls, roteadores, switches e balanceadores; d) Workstations."
19	**Análise de comportamento** A solução deverá ter critérios de avaliação de no mínimo das seguintes características de acesso: a) Acesso incomum a um dispositivo; b) Acesso de origem incomum; c) Acesso incomum a uma credencial; d) Acesso de duração incomum; e) Acesso de horário incomum." A solução deve permitir monitoramento em tempo real das sessões ou atividades dos usuários privilegiados, disponibilizada em interface centralizada (Dashboard).
20	**Acesso remoto seguro** A solução deve oferecer um link individual de uso temporário para que usuários possam realizar o acesso; A solução deve fornecer acesso limitado para usuários terceiros, onde possam apenas iniciar sessões em dispositivos pré aprovados;

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

	A solução deve prover acesso sem a necessidade do uso de VPN's no computador do usuário final;
21	**Dimensionamento da solução** Suportar, no mínimo, 3.000 sessões simultâneas; Suportar, no mínimo, 650.000 horas de armazenamento de gravação de sessões.
22	**Possuir recursos para implementar fluxo de aprovação para autorização (por email ou SMS)** A solução deve oferecer recursos para implementar um fluxo (workflow) de aprovação de novas autorizações quando necessário, enviando e-mail aos administradores ou usuários por eles delegados, para as as atividades de manutenção durante o ciclo de vida das contas.
23	**Possuir recursos de análise proativa de ameaças.** A solução deve oferecer relatórios e indicações automatizadas, de forma proativa, de possíveis ameaças e irregularidades no uso das sessões por ela protegidas. Tal funcionalidade deve ser amplamente configurável em seu escopo e granularidade, tanto na aquisição como no tratamento das informações coletadas.
24.	**Alertas e notificações** Envio de alerta por SIEM de senhas que não estejam iguais ao cofre.
25.	**Gerenciamento de senhas** A solução deve permitir parametrização de políticas de segurança e força de senha pelo administrador do sistema, dentre as quais: conjunto de caracteres alfanuméricos, numéricos e caracteres especiais, podendo ser escolhidos também quais caracteres especiais serão permitidos, com possibilidade de não possibilitar caracteres repeditos, gerando senhas aleatórias.
26.	**Integração** Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.
27.	**Integração com ferramentas de gestão** A Solução deve permitir integração com ferramentas de gestão de incidentes (ITSM) para validar tickets abertos durante processo de aprovação de acesso
28.	**Integração com SDK ou API** Ser disponibilizada um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações clientes possam: a) Solicitar credenciais e dispositivos;

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

	b) Cadastro e alteração credenciais e dispositivos; c) Solicitar chaves SSH; d) Cadastro e alteração de chaves SSH.
29.	**Cadastramento** Cadastro de equipamentos parametrizado manualmente
30.	**Licenciamento** O modelo de licenciamento da aplicação não deve restringir seu uso em caso do atingimento do limite das licenças contratadas;
31.	**Cadastramento de dispositivos** Atributos como Marca, Modelo, Fabricante, Localidade, Grupo abertos para configuração do administrador da ferramenta independente do fabricante. Cofre de Informações privilegiadas a) Armazenamento de certificados digitais; b) Armazenamento de senhas pessoais; c) Alerta de vencimento de informações armazenadas; d) Logs de alteração de informações privilegiadas; e) Permissão para compartilhamento de informações com outros usuários.
32.	**Relatórios** Relatórios de operação com lista de usuários, equipamentos e credenciais cadastradas;
33	**Segurança dos dados armazenados no cofre** Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;

4. Leia - se

ANEXO I – ESPECIFICAÇÃO TÉCNICA SOLUÇÃO

	ANEXO I - ESPECIFICAÇÃO TÉCNICA SOLUÇÃO
SUBITEM	**FUNCIONALIDADE**

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

Requisitos Funcionais Obrigatórios	
01	**Oferecer acesso segmentado (especificidade usuário + senha)** A solução de cofre de senhas deve permitir a definição detalhada dos privilégios (granularidade) concedidos a um usuário ou grupo específico no ativo ou recurso protegido. Apenas administradores da solução ou usuários por ele delegados poderão efetuar a inclusão, alteração e exclusão destes privilégios.
02	**Dispor de integração ao Microsoft Active Directory e serviço LDAP** A solução de cofre de senhas deve permitir a autenticação de usuários em domínios Microsoft Active Directory e serviços de diretório no padrão LDAP, de forma integrada e transparente, observando as características de grupamento destes usuários (unidade organizacional/OU). Necessário suportar estes servidores e domínios nas versões especificadas no **quadro 2 (Integração com ativos e produtos utilizados na MTI).**
03	**Dispor de cofre de senhas inacessível ao usuário final e não-legível para além do domínio da aplicação** A solução de cofre de senhas deve manter o conjunto de senhas (tanto de usuários finais como dos ativos e recursos protegidos) em estado criptografado, inacessível aos usuários finais e aos próprios ativos e recursos protegidos, em uma base que não possa ser utilizada caso copiada para além da própria solução. Todavia, deve dispor de uma forma segura para manter cópias de segurança das contas e configurações da solução.
04	**Efetuar registro individual do acesso por usuário (ainda que para um único par usuário/senha de um ativo/recurso protegido)** Ainda que o acesso ao ativo/recurso protegido se dê por um único par usuário/senha, a solução deve prover um registro individual por usuário final nela autenticado, a cada sessão. Este registro deverá indicar o período em que o usuário final manteve esta sessão e sua identidade, no mínimo, com fins de manter a rastreabilidade e a pessoalidade das sessões autenticadas.
5.	**Possuir capacidade de fornecer dados de acesso a aplicações e bancos de dados de forma segura.** A solução será capaz de fornecer acesso a aplicações desenvolvidas nas tecnologias e ambientes utilizados na empresa descritos no **quadro 2 (Integração com ativos e produtos utilizados na MTI),** seja entre aplicações ou entre estas e as soluções de bancos de dados listadas no mesmo quadro. Assim, a obtenção dos dados de

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

	autenticação entre as aplicações para troca de informações, ou para o acesso ao banco de dados, será efetuado através da solução de cofre de senhas, não exigindo dos desenvolvedores e mantenedores das aplicações o conhecimento das reais contas e senhas utilizadas nestes ativos/recursos protegidos.
6.	**Deve automatizar o ciclo de vida das contas e senhas geradas para os ativos protegidos, bem como permitir a gestão simplificada do ciclo de vida das contas e senhas dos usuários finais, através de políticas definíveis.** O ciclo de vida das senhas será automatizado (criação, renovação, expiração, rotação) de forma transparente e gerenciável, fazendo uso de senhas geradas randomicamente se assim requisitado, com a complexidade e periodicidade definidas por políticas configuráveis. Igualmente, deve permitir a gestão simplificada do ciclo de vida das contas e senhas dos usuários finais, também sujeitando-as a políticas configuráveis, quanto à sua criação, duração, renovação, expiração e exclusão. A definição destas políticas deve ser restrita aos administradores da solução ou aos usuários por eles delegados a esta função.
7.	**Prover recursos de auditoria e rastreabilidade do uso das credenciais** A solução proverá trilhas de auditoria, visando a rastreabilidade das ações executadas nas sessões por ela autenticadas. Os registros de auditoria e log devem ser invioláveis, sendo possível definir qual sua granularidade de acordo com a sessão e o usuário ou grupo de usuários autenticados, através de políticas configuráveis. Estas trilhas de auditoria devem ser armazenadas em formato criptografado, e deve ser garantida sua inviolabilidade e sua acessibilidade apenas aos administradores da solução ou usuários por eles delegados.
08.	**Possuir aderência da própria ferramenta e auxiliar na obtenção da aderência do conjunto de ativos e recursos protegidos à legislação nacional.** Deve implementar e auxiliar a implementar nas aplicações e ambiente protegidos pela solução à legislação nacional (LGPD, Lei Federal Brasileira nº 13709 de 2018).
9.	**Deve oferecer formas de single-sign-on, login único para mais de um recurso ou ativo protegido** Deve oferecer recursos de single-sign-on, onde uma única autenticação na solução de cofre de senhas permitiria o login seguro, identificado e rastreável, aos ativos protegidos habilitados para determinado usuário final. A partir desta autenticação, as sessões nos ativos e recursos protegidos irão se desenvolver conforme as permissões e políticas configuradas, tanto para o ativo/recurso específico como para o usuário autenticado.

Fones: +55 65 3613-3012/3056
PALÁCIO PAIAGUÁS - CENTRO POLÍTICO ADMINISTRATIVO - CPA
78050-970 - CUIABÁ - MATO GROSSO

10.	**Possuir recursos de análise proativa de ameaças.** A solução deve oferecer relatórios e indicações automatizadas, de forma proativa, de possíveis ameaças e irregularidades no uso das sessões por ela protegidas. Tal funcionalidade deve ser amplamente configurável em seu escopo e granularidade, tanto na aquisição como no tratamento das informações coletadas.
11.	**Implementar gestão da identidade do usuário final com recursos de autenticação em duas etapas (2FA)** Deve disponibilizar recursos de duplo fator de autenticação para o usuário final, nas formas de mensagem de e-mail, SMS, aplicação para smartphone nos padrões Android e IOS. O código (token) enviado deve possuir tempo de vida pré-determinado, e a exigência de autenticação por duplo fator deve ser configurável na política de autenticação para cada recurso/ativo protegido.

* Permanecem inalteradas as demais cláusulas do Edital.

ALCI DE OLIVEIRA JUNIOR:83080163168
Assinado de forma digital por ALCI DE OLIVEIRA JUNIOR:83080163168
Dados: 2022.11.09 11:03:56 -04'00'

Cuiabá-MT, 08 de novembro de 2022

Alci de Oliveira Junior
Gerente da Unidade de Gestão de Aquisições e Contratos

CLEBERSON ANTONIO SAVIO GOMES:80180663100
Assinado digitalmente por CLEBERSON ANTONIO SAVIO GOMES:80180663100
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=VALID, OU=AR ONLINE SOLUCOES DIGITAIS, OU=Videoconferencia, OU=11587975000184, CN=CLEBERSON ANTONIO SAVIO GOMES:80180663100
Razão: Eu sou o autor deste documento
Localização:
Data: 2022-11-09 14:31:32
Foxit Reader Versão: 9.3.0

CLEBERSON ANTÔNIO SÁVIO GOMES
DIRETOR PRESIDENTE INTERINO DA MTI